Pow and pos

Synopsis:

* Introduction
* Blockchain
* Proof of work
* Benefits of pow
* Proof of stake
* Benefits of pos
* Hybrid approach
* Conclusion

Proof of work:

A  **proof-of-work** (**PoW**) **system** (or **protocol**, or **function**) is a [consensus mechanism](https://en.wikipedia.org/wiki/Consensus_(computer_science)). It deters [denial-of-service attacks](https://en.wikipedia.org/wiki/Denial-of-service_attack) and other service abuses such as [spam](https://en.wikipedia.org/wiki/Spam_(electronic)) on a network by requiring some work from the service requester, usually meaning processing time by a computer. The concept was invented by [Cynthia Dwork](https://en.wikipedia.org/wiki/Cynthia_Dwork) and [Moni Naor](https://en.wikipedia.org/wiki/Moni_Naor) as presented in a 1993 journal article.[[1]](https://en.wikipedia.org/wiki/Proof_of_work#cite_note-DwoNao1992-1) The term "proof of work" was first coined and formalized in a 1999 paper by [Markus Jakobsson](https://en.wikipedia.org/wiki/Markus_Jakobsson) and Ari Juels. A key feature of these schemes is their asymmetry: the work must be moderately hard (yet feasible) on the requester side but easy to check for the service provider. This idea is also known as a CPU cost function, [client puzzle](https://en.wikipedia.org/wiki/Client_Puzzle_Protocol), computational puzzle, or CPU pricing function. It is distinct from a [CAPTCHA](https://en.wikipedia.org/wiki/CAPTCHA), which is intended for a human to solve quickly, while being difficult to solve for a computer. **Proof-of-Work**, or PoW, is the original consensus algorithm in a **Blockchain** network. In **Blockchain**, this algorithm is used to confirm transactions and produce new blocks to the chain. With PoW, miners compete against each other to complete transactions on the network and get rewarded.

Benefits of pow:

 A Proof of Work system is one that forces computers to do a little extra work before a requested process is executed. The extra work results in a solution, which is then presented to the other computers in a network. The other computers can easily verify that the solution is accurate and approve whatever action the original computer is requesting.

This is a key characteristic of a Proof of Work system: it must be somewhat difficult to find a solution but extremely easy to verify that a particular answer does, in fact, solve the problem. [Cryptographic hash functions](https://komodoplatform.com/cryptographic-hash-function/) play a huge role in modern Proof of Work implementations. In this way, Proof of Work systems are similar to [Merkle Trees](https://komodoplatform.com/whats-merkle-tree/" \t "_blank). Once a hash is created, all other machines can verify that it is a true result with very little computational effort.

There are several major benefits to Proof of Work systems. First, they are an excellent way to deter spammers. If a moderate amount of work is required for each process (e.g. sending an email), then most spammers wouldn’t have enough computational power to send a huge number of unsolicited emails.

Or, in the case that a spammer did have enough computational power to send a huge number of emails, the financial costs of this processing power (i.e. buying the hardware and paying for the electricity) would likely exceed the profits to made from spamming. That’s how a Proof of Work system disincentivizes spamming and other forms of malicious behavior.

In addition, Proof of Work systems can be used to provide security to an entire network. This is the primary benefit for blockchains that use a Proof of Work consensus mechanism. If enough nodes (computers or dedicated mining machines) are competing to find a specific solution, then the computational power needed to overpower and manipulate a network becomes unattainable for any single bad actor or even a single group of bad actors.

Proof of stake:

**Proof of stake** (**PoS**) is a type of [consensus algorithm](https://en.wikipedia.org/wiki/Consensus_(computer_science)) by which [cryptocurrency](https://en.wikipedia.org/wiki/Cryptocurrency) [blockchain](https://en.wikipedia.org/wiki/Blockchain_(database)" \o "Blockchain (database)) network aims to achieve [distributed consensus](https://en.wikipedia.org/wiki/Consensus_(computer_science)). In PoS-based cryptocurrencies the creator of the next block is chosen via various combinations of random selection and wealth or age (*i.e.,* the stake). In contrast, the algorithm of [proof-of-work](https://en.wikipedia.org/wiki/Proof-of-work_system)-based cryptocurrencies such as [bitcoin](https://en.wikipedia.org/wiki/Bitcoin) uses [mining](https://en.wikipedia.org/wiki/Bitcoin_network#Mining); that is, the solving of computationally intensive puzzles to validate transactions and create new blocks.Proof of stake must have a way of defining the next valid block in any blockchain. Selection by account balance would result in (undesirable) centralization, as the single richest member would have a permanent advantage. Instead, several different methods of selection have been devised. Proof of Stake (PoS) concept states that a person can mine or validate block transactions according to how many coins he or she holds. This means that the more [Bitcoin](https://www.investopedia.com/terms/b/bitcoin.asp) or [altcoin](https://www.investopedia.com/terms/a/altcoin.asp) owned by a miner, the more mining power he or she has.

Benefits of pos:

Incentives differ between the two systems of block generation. Under [proof of work](https://en.wikipedia.org/wiki/Proof_of_work), miners may potentially own none of the currency they are mining and thus seek only to maximize their own profits. It is unclear whether this disparity lowers or raises security risks. Under proof of stake, however, those "guarding" the coins always own the coins, although several cryptocurrencies do allow or enforce the lending of staking power to other nodes.  **Proof of Work** rewards its miner for solving complex equations, in **Proof of Stake**, the individual that creates the next block is based on how much they have 'staked'. To make things simple for you, the **stake** is based on the number of coins the person has for the particular blockchain they **are** attempting to mine.

Hybrid approach:

Hybrid is combination of pow and pos such that a person can get profit doubled .If we combine these two then we can get huge profit because in case of pow the miners with more energy solves the puzzle at greater speed and in case of pos we can get huge profit by storing the money eanred by pow.If we keep it for a long time we can increase the amount percentage. For example if we have 40% at present if we use use pow we make our percent to reach 51%. If we apply pos to this we can make it as double by storing this and earn money by using pow further and further. Even if we have a loss in anyone of these we can regain it with another one.For example if we get a loss in POW we can compensate it with the POS such that we will not get losses eventhough we detrive ours respectively. If we invest 25% in mining business and we got a profit of 25% by using POW then we can double the profit by using pos instead of going again with pow. But if we store more money by pos it is considered as illegal and he/she would be penalised with some amount from their percent of stake. In this we can huge benefit of percentage. This is one of the main benefits of this hybrid approach.but the major disadvantage is that eventhough we got a huge profit by this combination we should invest further in work or the percentage of our share will be detrived and we will be penalised according to the rules.